CompTIA Cybersecurity Analyst (CySA+) Certification

Audience

CompTIA Cybersecurity Analyst (CySA+) is an IT workforce certification that applies behavioral analytics to networks and devices to prevent, detect and combat cybersecurity threats through continuous security monitoring. It is aimed at:

- Security analysts
- Security engineers
- Incident response
- Threat hunters
- Threat intelligence analysts
- Application security analysts
- Compliance analysts

Prerequisites

While there are no required prerequisites, the following are recommended:

- CompTIA Network+ Certification, or equivalent knowledge.
- CompTIA Security+ Certification, or equivalent knowledge.
- 4 years of hands-on information security or related experience.

Duration

5 days

Course Objectives

As attackers have learned to evade traditional signature-based solutions, such as firewalls and anti-virus software, an analytics-based approach within the IT security industry is increasingly important for organizations. CompTIA CySA+ applies behavioral analytics to networks to improve the overall state of security through identifying and combating malware and advanced persistent threats (APTs), resulting in an enhanced threat visibility across a broad attack surface. It will validate an IT professional’s ability to proactively defend and continuously improve the security of an organization. CySA+ will verify the successful candidate has the knowledge and skills required to:

- Leverage intelligence and threat detection techniques
- Analyze and interpret data
- Identify and address vulnerabilities
- Suggest preventative measures
- Effectively respond to and recover from incidents

CompTIA CySA+ is the only intermediate high-stakes cybersecurity analyst certification with both hands-on, performance-based questions and multiple-choice questions.

CySA+ focuses on the candidates ability to not only proactively capture, monitor, and respond to network traffic findings, but also emphasizes software and application security, automation, threat hunting, and IT regulatory compliance, which affects the daily work of security analysts.

CySA+ covers the most up-to-date core security analyst skills and upcoming job skills used by threat intelligence analysts, application security analysts, compliance analysts, incident responders/handlers, and threat hunters, bringing new techniques for combating threats inside and outside of the Security Operations Center (SOC).

CompTIA CySA+ meets the ISO 17024 standard and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA). Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

What Skills Will You Learn?

- Threat and Vulnerability Management
  - Utilize and apply proactive threat intelligence to support organizational security and perform vulnerability management activities.
- Security Operations and Monitoring
  - Analyze data as part of continuous security monitoring activities and implement configuration changes to existing controls to improve security.
- Software and Systems Security
  - Apply security solutions for infrastructure management and explain software and hardware assurance best practices.
- Incident Response
  - Apply the appropriate incident response procedure, analyze potential indicators of compromise, and utilize basic digital forensics techniques.
- Compliance and Assessment
  - Apply security concepts in support of organizational risk mitigation and understand the importance of frameworks, policies, procedures, and controls.

Course Content

Threat and Vulnerability Management

Explain the importance of threat data and intelligence
Intelligence sources
Confidence levels
Indicator management
Threat classification
Threat actors
Intelligence cycle
Commodity malware
Information sharing and analysis communities

Given a scenario, utilize threat intelligence to support organizational security
Attack frameworks
Threat research
Threat modeling methodologies
Threat intelligence sharing with supported functions

Given a scenario, perform vulnerability management activities
Vulnerability identification
Validation
Remediation/mitigation
Scanning parameters and criteria
Inhibitors to remediation

Given a scenario, analyze the output from common vulnerability assessment tools
Web application scanner
Infrastructure vulnerability scanner
Software assessment tools and techniques
Enumeration
Wireless assessment tools
Cloud infrastructure assessment tools

Explain the threats and vulnerabilities associated with specialized technology
Mobile
Internet of Things (IoT)
Embedded
Real-time operating system (RTOS)
System-on-Chip (SoC)
Field programmable gate array (FPGA)
Physical access control
Building automation systems
Vehicles and drones
Workflow and process automation systems

Industrial control system
Supervisory control and data acquisition (SCADA)

Explain the threats and vulnerabilities associated with operating in the cloud

Cloud service models
Cloud deployment models
Function as a Service (FaaS)/serverless architecture
Infrastructure as code (IaC)
Insecure application programming interface (API)
Improper key management
Unprotected storage
Logging and monitoring

Given a scenario, implement controls to mitigate attacks and software vulnerabilities

Attack types
Vulnerabilities

Software and Systems Security

Given a scenario, apply security solutions for infrastructure management

Cloud vs. on-premises
Asset management
Segmentation
Network architecture
Change management
Virtualization
Containerization
Identity and access management
Cloud access security broker (CASB)
Honeypot
Monitoring and logging
Encryption
Certificate management
Active defense

Explain software assurance best practices

Platforms
Software development life cycle (SDLC) integration
DevSecOps
Software assessment methods
Secure coding best practices
Static analysis tools
Dynamic analysis tools
Formal methods for verification of critical software
Service-oriented architecture

Explain hardware assurance best practices

Hardware root of trust
eFuse
Unified Extensible Firmware Interface (UEFI)
Trusted foundry
Secure processing
Anti-tamper
Self-encrypting drive
Trusted firmware updates
Measured boot and attestation
Bus encryption

Security Operations and Monitoring

Given a scenario, analyze data as part of security monitoring activities

Heuristics
Trend analysis
Endpoint
Network
Log review
Impact analysis
Security information and event management (SIEM) review
Query writing
E-mail analysis

Given a scenario, implement configuration changes to existing controls to improve security

Permissions
Whitelisting
Blacklisting
Firewall
Intrusion prevention system (IPS) rules
Data loss prevention (DLP)
Endpoint detection and response (EDR)
Network access control (NAC)
Sinkholing
Malware signatures
Sandboxing
Port security

Explain the importance of proactive threat hunting

Establishing a hypothesis
Profiling threat actors and activities
Threat hunting tactics
Reducing the attack surface area
Bundling critical assets
Attack vectors

Integrated intelligence
Improving detection capabilities

Compare and contrast automation concepts and technologies

Workflow orchestration
Scripting
Application programming interface (API) integration
Automated malware signature creation
Data enrichment
Threat feed combination
Machine learning
Use of automation protocols and standards
Continuous integration
Continuous deployment/delivery

Incident Response

Explain the importance of the incident response process

Communication plan
Response coordination with relevant entities
Factors contributing to data criticality

Given a scenario, apply the appropriate incident response procedure

Preparation
Detection and analysis
Containment
Eradication and recovery
Post-incident activities

Given an incident, analyze potential indicators of compromise

Network-related
Host-related
Application-related

Given a scenario, utilize basic digital forensics techniques

Network
Endpoint
Mobile
Cloud
Virtualization
Legal hold
Procedures
Hashing
Carving
Data acquisition

Compliance and Assessment

Understand the importance of data privacy and protection
Privacy vs. security
Non-technical controls
Technical controls

Given a scenario, apply security concepts in support of organizational risk mitigation
Business impact analysis
Risk identification process
Risk calculation
Communication of risk factors
Risk prioritization
Systems assessment
Documented compensating controls
Training and exercises
Supply chain assessment

Explain the importance of frameworks, policies, procedures, and controls
Frameworks
Policies and procedures
Category
Control type
Audits and assessments